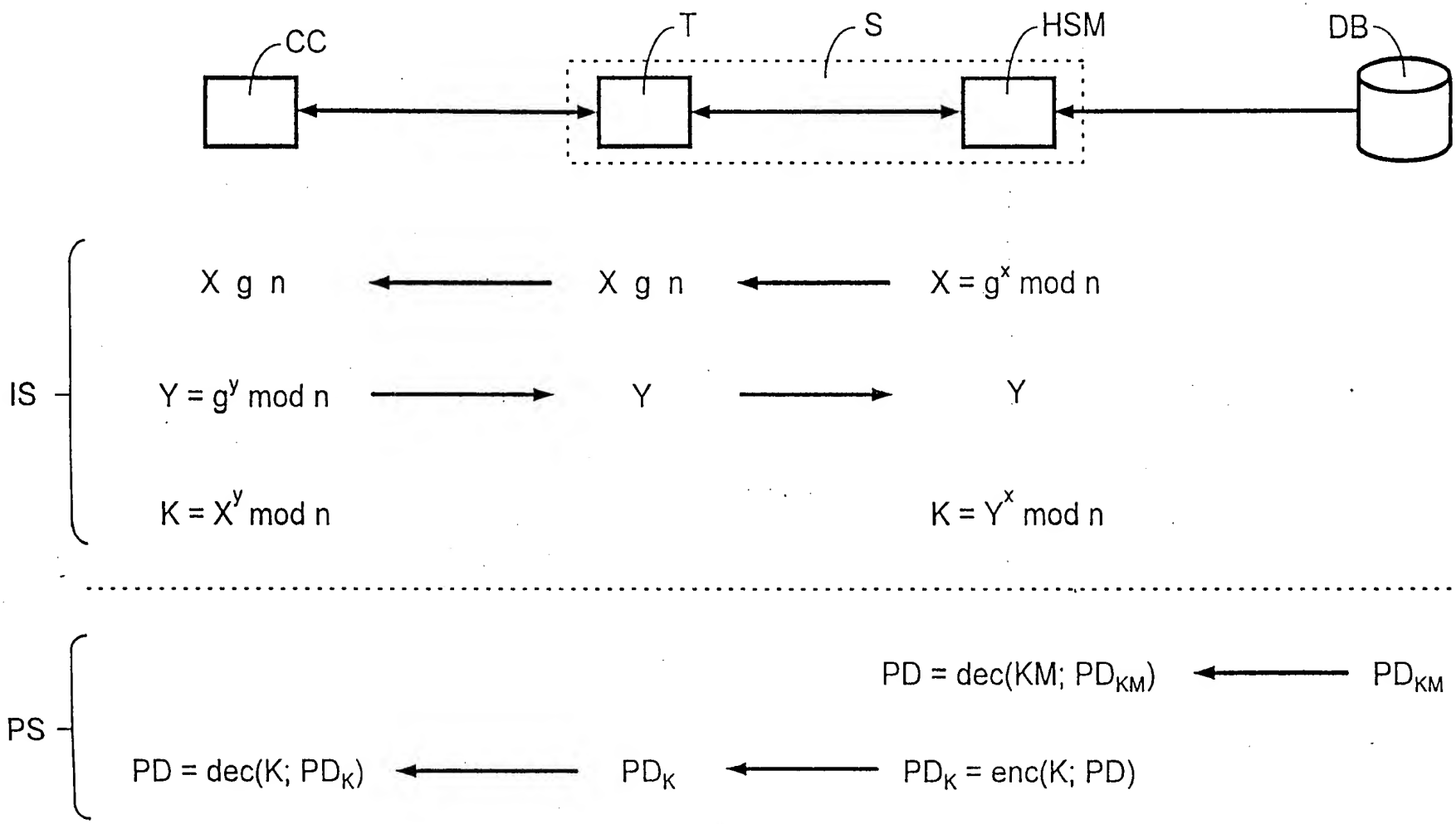
CC
T
S
HSM
DB
IS
X g n
X g n
X = g^x mod n
Y = g^y mod n
Y
Y
K = X^y mod n
K = Y^x mod n
PS
PD = dec(KM; PD_KM)
PD_KM
PD = dec(K; PD_K)
PD_K
PD_K = enc(K; PD)

Fig.